FENWICK

555 California Street
12th Floor
San Francisco, CA 94104

415.875.2300
Fenwick.com

Tyler G. Newby
tnewby@fenwick.com | 415.875.2495

December 6, 2021

VIA EMAIL (BKLEIN@WAYMAKERLAW.COM)

Brian Klein
Waymaker LLP
777 S. Figueroa Street, Suite 2850
Los Angeles, CA 90017

Re: United States v. Thompson, CR19-159RSL (Amazon Ref. No. CRIM1111531)

Dear Brian:

As you requested during our call to meet and confer regarding the referenced subpoena, I am writing to confirm the requests on which we have reached agreements and those where we have not.

Request 1: Any documents and communications relating to the Company's knowledge or awareness on or before March 12, 2019 of any misconfigurations of its cloud infrastructure, including any misconfigurations of the web application firewalls (or "WAFs") utilized by the Company and/or its customers, including Capital One Financial Corporation ("Capital One"), [redacted]

As we have stated in our previous correspondence, AWS is not aware of any documents responsive to this request, nor is AWS's knowledge of any of its customers' misconfigurations relevant to the case. You requested that Amazon provide excerpts of a corporate representatives' testimony from In re: Capital One Consumer Data Breach Litigation, Case No.: 19-cv-2947-AJT-JFA, in the Eastern District of Virginia on Amazon's lack of knowledge of its customers' configurations of the WAFs they use in their AWS accounts. AWS agrees to provide you excerpts of that testimony pursuant to a protective order.

Request 2: Any documents and communications involving anyone in the Company's Office of the Chief Information Security Officer relating to Paige Thompson's alleged exploitation of the Company's misconfigurations of its cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or its customers.

As stated in Amazon's September 21, 2021 letter to you, AWS agrees to produce documents from within its security organization concerning the root cause – how the exploit was carried out and what was accessed – of your client's access of AWS customers' accounts

through August 5, 2019. These documents will include tickets of the security operations teams investigation and communications (if any) with affected customers. With respect to materials subject to the attorney-client or work product privileges, AWS will provide a log of documents that are wholly withheld and will redact privileged materials contained within documents that it produces that also consist of non-privileged materials.

Request 3. Any discovery-related correspondence, requests, and responses in Case No.: 19-cv-2947-AJT-JFA, in the Eastern District of Virginia. For example, this would include all of the Company's responses to requests for admissions or interrogatories, as well as letters discussing objections to discovery requests or productions of discovery.

As agreed, AWS will produce its interrogatory responses from the civil litigation describing the incident.

Request 4. Any unsolicited security advice related to reports of vulnerabilities of the Company's cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or its customers from March 12, 2019 through the present. For example, this would include reports from "white hats" or security researchers to the Company about any type of misconfigurations of its cloud infrastructure.

AWS will produce non-privileged documents and communications with Capital One about a note that was handed to an AWS security engineer at a May 2019 conference that referenced a potential vulnerability associated with a specific IP address used by Capital One. Otherwise, this request is overly broad and is not relevant, and AWS will not produce documents in response to it.

Request 5. Any communications involving anyone in the Company's Office of the Chief Information Security Officer or any Executive Officers (e.g., CEO, CFO, GC, and CIO) of the Company with anyone at Capital One relating to (a) any misconfigurations of its cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or Capital One; and/or (b) Paige Thompson from March 12, 2019 until present.

This request overlaps with Request 2. As stated in Amazon's September 21 letter, AWS agrees to produce documents from its ticketing system that contain investigation notes and communications (if any) with customers other than Capital One that were impacted by your client's conduct.

Request 6. Any documents and communications from April 1, 2019 through the present relating to a bug bounty program for the Company tied the Company's [sic] misconfiguration of its cloud infrastructure, including any misconfigurations of the WAFs

utilized by the Company or its customers. For example, this would include its Vulnerability Research Program discussed on hackerone.com.

As stated in Amazon's May 18, 2021 letter to you, there was no misconfiguration of AWS's cloud infrastructure relating to this breach. Moreover, AWS's bug bounty program does not encompass customer misconfigurations.

Request 7. Any documents and communications from March 12, 2019 through present relating to the reasons why AWS developed and launched AWS EC2 instance metadata service ("IMDS") version 2, also known as IMDSv2.

As we have explained in prior correspondence and in our call, this request is impermissibly overbroad and is not relevant. AWS will not produce documents in response to this request.

Request 8. Any contracts relating to cloud infrastructure and/or WAFs between the Company and one of the following parties: Capital One, [redacted]

As we have explained in prior correspondence, the terms of AWS's commercial agreements with its customers are irrelevant to your client's guilt or innocence. AWS will not produce the requested agreements.

Request 9. Any bills and invoices for providing cloud infrastructure from January 1, 2019 through December 31, 2020 sent from the Company to the following entities: AWS, Capital One, [redacted]

As stated in our prior correspondence AWS's invoices and billing to these customers is irrelevant to your client's guilt or innocence and would not be useful at sentencing. AWS will not produce documents in response to this request.

* * *

Finally, we need to finalize the protective order prior to AWS's production of the items it agrees to produce. Please send a final version that incorporates the revisions in the redline version you sent to Amazon on October 29, 2021, a copy of which is attached.

Sincerely,

FENWICK & WEST LLP

Tyler G. Newby